Neformální úvod do formální matematiky

Jakub Smolík

26. prosince 2023

Obsah

1 Trocha historie

V matematice je stejně jako ve všech vědních oborech velmi zajímavá historie; jak se jednotlivé disciplíny vyvíjely v čase a jaké byly motivace pro různé objevy. Teorie množin je tak trochu výjimka, protože nemá počátky už v dávných dobách antiky, ani ji neobjevilo více lidí nezávisle na sobě. Prvotní myšlenka totiž pocházela od jediného člověka, a sice Georga Cantora (1845–1918), který svůj první článek o teorii množin publikoval roku 1874.

Cantor představil teorii množin jako způsob, jak studovat nekonečné objekty. Matematici se ode vždycky nekonečna strašně báli a snažili se mu vyhýbat jako čert kříži, ale stejně na ně vždycky někde zase vykouklo. Cantor nejenom ukázal, že nekonečné objekty je možné popsat, ale dokonce, že nekonečen je svým způsobem nekonečně mnoho různých druhů. Tohle bylo v té době neuvěřitelně kontroverzní, ale postupem času se s tím matematici smířili.

Dalším důvodem pro vznik teorie množin byla snaha sjednotit základy různých matematických oborů. Matematika ve středověku a v raném novověku byla z dnešního pohledu strašný chaos. Různá její odvětví se vyvíjela zcela nezávisle na sobě a neměla žádný společný teoretický základ. Ono to vlastně nevadilo, protože např. teorii grafů můžete bez problémů studovat, aniž byste měli graf definovaný množinově, stačí vám nějaká geometrická interpretace vrcholů spojených hranami. Geometrická interpretace byla všude prominentní, protože je intuitivní, velmi efektivní a většinou funguje. A tady je zakopaný pes. Jednou z nejdůležitějších disciplín matematiky je takzvaná matematická analýza, která ve své nejzákladnější podstatě studuje chování funkcí jedné proměnné. Její počátky sahají už do starověku, ale opravdu velké objevy v ní se udály až v 17. století. Jedni z nejdůležitějších matematiků tohoto období jsou Newton a Leibniz, kteří nezávisle na sobě vyvinuli infinitesimální počet. Ten využíval nekonečně malých hodnot a byl založený na geometrické interpretaci reálných čísel jako spojité přímky. Leibniz svoje objevy publikoval roku 1684, zatímco Newton až v roce 1687. Newton byl ovšem velký tajnůstkář a kalkulus zřejmě vynalezl už v v letech 1665-1666, když si pohrával s myšlenkou gravitace. Leibnize obvinil, že si objev kalkulu přivlastnil a desítky let se s ním handrkoval.

Všechno v analýze fungovalo naprosto perfektně až do roku 1872. Karl Weierstrass tehdy publikoval článek, ve kterém představil tak odpornou funkci, že kompletně rozbila všechno, co se do té doby v analýze objevilo. Tato funkce, v dnešní době známa jako Weierstrassova, je totiž spojitá všude, ale nikde nemá derivaci, což kompletně rozbíjí jakoukoli geometrickou představu o funkcích. Bylo tedy potřeba všechno vybudovat od znovu, tentokrát pořádně a za použití exaktních struktur. Ne geometrické interpretace.

Matematici Bertrand Russell a Gottlob Frege chtěli pomocí teorie množin pořádně definovat čísla. Používáme je tak běžně a samozřejmě, že se nikdy nezamyslíme nad tím, co vlastně jsou. Jejich myšlenka byla následující: „Co je esencí čísla 4? To, že vždy popisuje nějaké čtyři objekty.“ Dobře, tak prostě řekneme, že číslo 4 je nějaký soubor všech čtveřic objektů. V teorii množin bychom řekli, množina všech čtyř-prvkových množin. Ovšem okolo roku 1900 se ukázalo, že tohle se také rozbije.

Matematici se ovšem nevzdali a během dalších přibližně dvaceli let vzniklo něco, co dnes známe pod názvem ZFC. Jde o formální, axiomatickou teorii množin,

kde nevznikají takové paradoxy jako v Cantorově původní, naivní teorii množin.

Položit společný základ pro matematiku, se tedy nakonec přes všechny zádrhele podařilo, protože v dnešní době je v matematice všechno definované jako množina.

2 Jazyk matematiky

Matematika se po staletí popisovala téměř výhradně přirozeným jazykem. Ještě v nějakém 15. století prakticky neexistovala žádná matematická notace a všechno se psalo slovně. Všechny tvrzení, důkazy, rovnice atd. Fungovalo to, ale z dnešního pohledu to bylo absurdně neefektivní. Zdá se až neuvěřitelné, jak daleko se matematici dokázali dostat pouze s přirozeným jazykem. Nicméně jak se koncepty v matematice stávaly čím dál komplikovanější a matematický svět byl čím dál propojenější, tak se postupem času vyvinul nějaký jazyk matematiky, který nehovoří ve slovech, ale ve speciálních symbolech. Samozřejmě to neznamená, že se přirozený jazyk už nepoužívá, potom by se v tom nikdo nevyznal. V této kapitole si stručně představíme jazyk matematiky, protože jej budeme v ostatních kapitolách hojně využívat.

2.1 Logika

Nejprve si neformálně představíme základní pojmy výrokové a predikátové logiky. Logika je věda o formální správnosti myšlení. Formálně logická správnost spočívá ve správnosti vyvození závěru z předpokladů.

- **Výrok** je jakékoli tvrzení, o němž má smysl říci, že platí nebo že neplatí. Například „Venku prší“ je výrok, ale „Prší venku?“ výrok není.
  - **Tautologie** je výrok, který je vždy pravdivý. Příklad tautologie je „*Venku prší nebo venku neprší.*“
  - **Spor** je výrok, který je vždy nepravdivý. Příklad sporu je „*Venku prší právě tehdy, když venku neprší.*“
- **Negace** $\neg A$ výroku A je výrok „*Není pravda, že platí A.*“
- **Konjunkce** $A \wedge B$ výroků A a B je výrok „*Platí A i B.*“
- **Disjunkce** $A \vee B$ výroků A a B je výrok „*Platí A nebo B.*“
- **Implikace** $A \Rightarrow B$ je výrok „*Pokud platí A, potom platí i B.*“ Výrok A je **postačující podmínkou** pro platnost B a B je **nutnou podmínkou** pro platnost A.

  Podívejme se třeba na implikaci „*Když prší, tak je mokro.*“ Mokro může být i když neprší, například pokud někdo rozlije vodu, takže déšť je *postačující* pro mokro. Na druhou stranu se nikdy nemžuže stát, že by pršelo, ale venku nebylo mokro. Mokro je tedy *nutné* aby mohla být pravda, že prší.
- **Ekvivalence** $A \Leftrightarrow B$ je výrok „*Výrok A platí tehdy a jen tehdy, když platí výrok B.*“ Všimněme si, že výrok $(A \Rightarrow B) \wedge (B \Rightarrow A)$ má stejný význam.
- **Pravdivostní hodnota** výroku je 1, pokud je pravdivý, a 0, pokud není.

  Zamysleme se nad pravdivostní hodnotou složených výroků. Aby byl výrok „*Vánočka je sladká i měkká.*“ pravdivý, tak *vánočka musí být sladká* a zároveň *vánočka musí být měkká*. Na druhou stanu, pro splnění tvrzení „*Vánočka je sladká nebo měkká.*“ stačí splnit libovolnou z těchto vlastností.

Jediný případ, kdy implikace „*Když prší, tak je mokro*“ není pravdivá, je, když prší, ale není mokro. Pokud neprší, tak je jedno, jestli tam je nebo není mokro, protože o tom tento výrok vůbec nehovoří.

A	$\neg A$
1	0
0	1

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Tabulka pravdivostních hodnot logických spojek.

- **Logická formule**[1] je výraz $\varphi(x_1,x_2,\dots x_n)$, z něhož vznikne výrok tím, že do něj dosadíme prvky $x_1 \in M_1, \dots x_n \in M_n$ z daných množin $M_1, \dots M_n$. Příklad výrokové formule s jednou volnou proměnnou je třeba

  $$\varphi(x) = x \textit{ je kladné sudé číslo.}$$

  Množinu si můžeme představovat jako nějakou skupinu objektů, které mají nějakou společnou vlastnost; například, že to jsou čísla. Zápis $x \in M$ značí, že x je prvkem množiny M.

- Nyní nechť $\varphi(x)$, $x \in M$ je logická formule.

  - Výrok „*Pro všechna* $x \in M$ *platí* $\varphi(x)$.“ zapisujeme jako $\forall x \in M : \varphi(x)$. Symbol $\forall$ se nazývá **obecný kvantifikátor**.
  - Výrok „*Existuje* $x \in M$*, pro které platí* $\varphi(x)$.“ zapisujeme jako $\exists x \in M : \varphi(x)$. Symbol $\exists$ se nazývá **existenční kvantifikátor**.
  - Výrok „*Existuje právě jedno* $x \in M$*, pro které platí* $\varphi(x)$.“ zapisujeme jako $\exists! x \in M : \varphi(x)$.

- **Axiom** je výrok, který považujeme za pravdivý a to, že je pravdivý, nedokazujeme. Příklad axiomu, který potkáme, je „Existuje prázdná množina.“

- **Věta** je zpravidla nějaký důležitý výrok, který se snažíme dokázat.

- **Lemma** je zpravidla pomocné tvrzení, které slouží k důkazu nějaké věty.

- **Důkaz** je proces, kdy se z axiomů a již dokázaných tvrzení snažíme ukázat pravdivost něčeho nového.

- **Teorie**[2] je nějaká množina axiomů. Nyní nechť T je teorie. Výrok A je

  1. **pravdivý** v T, pokud je jej možné dokázat z jejích axiomů,
  2. **lživý**, **nepravdivý** v T, pokud je v T pravdivá jeho negace,
  3. **nezávislý** v T, pokud jej z axiomů T není možné dokázat ani vyvrátit.

  To, že nějaký výrok není pravdivý, ještě neznamená, že je nepravdivý (lživý)!

[1] Také atomická formule, predikát nebo výroková forma.
[2] Pojem teorie je zde uvedený velmi zjednodušeně.

- Teorie je **sporná**, pokud je v ní pravdivý spor.

  Uvědomme si, že pokud je teorie sporná, potom je něco v nepořádku s jejími axiomy. Protože pokud jsme v důkazu tohoto sporu neudělali žádnou chybu, potom je implikace „*Konjunkce axiomů $T \Rightarrow$ spor.*“ pravdivá. Spor je vždy nepravdivý, takže tato implikace je pravdivá pouze tehdy, když je „*Konjunkce axiomů T*“ nepravdivá. To znamená, že s naší volbou axiomů je něco fundamentálně špatně, protože jsme předpokládali, že jsou všechny pravdivé.

Teorie množin, nemá v názvu slovo „teorie“ jen tak náhodou, ale protože to opravdu je teorie. Nejprve si představíme Cantorovu naivní teorii množin, ale ukáže se, že je sporná. Pokusíme se její axiomy změnit, aby tento spor nemohl vzniknout, což povede na Zermelovu-Fraenkelovu teorii množin. Není to ani zdaleka jediná teorie množin, která se pokouší opravit Cantorovu původní myšlenku, ale je dneska asi nejrozšířenější.

2.2 Značení číselných oborů

Následuje seznam běžného značení číselných oborů.

$\mathbb{N}$, $\mathbb{N}^+$	**přirozená čísla**: $0, 1, 2, 3, \ldots$ a přirozená čísla bez nuly
$[n]$	značí množinu přirozených čísel od 1 do n.
$\mathbb{Z}$	**celá čísla**: $0, 1, -1, 2, -2, 3, -3, \ldots$
$\mathbb{Q}$	**racionální čísla** neboli zlomky: $1, -2, \frac{3}{2}, -\frac{4}{7}, \ldots$
$\mathbb{R}$	**reálná čísla** jsou zlomky spolu s iracionálními čísly jako π nebo $\sqrt{2}$.
$\mathbb{R}^+$, $\mathbb{R}_0^+$	kladná reálná čísla, nezáporná reálná čísla.
$\mathbb{C}$	**komplexní čísla** jsou reálná čísla rozšířená o imaginární jednotku i.

2.3 Dva druhy rovnosti

Dále budeme rozlišovat dva druhy rovnosti a dva druhy ekvivalence.

$=$ je obyčejná rovnost určená k porovnávání věcí. Zápis $x = 2$ je logická formule, která je splněná právě tehdy, když x je rovno dvojce.

$:=$ je **definiční rovnost** určená k definování věcí. Zápis $x := 2$ je přiřazení čísla 2 do proměnné x. Vlastně tím deklarujeme, že odteď je x jen jiný symbol pro dvojku.

$\Leftrightarrow$ je logická spojka ekvivalence určená k vyrábění výroků.

$\equiv$ je **definiční ekvivalence** určená k definování nových vlastností. Zápis „$x \in \mathbb{Z}$ *je super* $\equiv \exists n \in \mathbb{N} : x = 2n$.“ definuje novou vlastnost „být super“. Podle této definice jsou sudá čísla super a lichá čísla nejsou super.

2.4 Notace velkých operátorů

V matematice se často setkáme s velkými operátory, které slouží k zpřehlednění zápisu. Například sumace se značí symbolem $\sum$. Tato notace se většinou používá dvěma způsoby. Buď jako suma přes všechna n od nějakého počátečního indexu po koncový nebo jako suma přes všechny prvky nějaké množiny:

$$\sum_{n=1}^{4} n^2 = 1^2 + 2^2 + 3^2 + 4^2, \qquad \sum_{k\in[n]} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{n^2}.$$

Podobně $\prod$ značí součin, $\bigcup$ sjednocení a $\bigcap$ průnik. Pokud potřebujeme udělat konjunkci nebo disjunkci mnoha výroků, tak můžeme použít operátory $\bigwedge$ a $\bigvee$.

3 Důkazové techniky

Při dokazování vycházíme z axiomů a již dokázaných tvrzení a snažíme se dokázat pravdivost něčeho nového. Nejdůležitější nástroj v arzenálu matematika jsou právě důkazové techniky, protože na různá tvrzení se často hodí různé přístupy. Neexistuje žádný univerzální způsob, jak dokázat všechno, co bychom chtěli. Důkaz je možné brát jako takovou hru pro dva hráče, kde se ten první snaží přesvědčit toho druhého, že to tvrzení je pravdivé a ten druhý mu do toho šťourá. Takže ten druhý může kdykoli ukázat na kterýkoli krok důkazu a říct „Tomuhle tak úplně nevěřím, to mi nepřijde triviální.“ a ten první by měl umět ten problémový krok rozepsat na ještě jednodušší kroky. Konec důkazu značíme symbolem □.

3.1 Přímý důkaz

I když to tak na první pohled třeba nevypadá, tak vždy dokazujeme nějakou implikaci $P \Rightarrow T$, kde P jsou předpoklady pro platnost T. Součástí předpokladů jsou i všechny axiomy naší teorie. Pokud bychom potřebovali dokázat nějakou ekvivalenci $A \Leftrightarrow B$, tak místo ní dokážeme dvě implikace $A \Rightarrow B$ a $B \Rightarrow A$. Přímý důkaz nevyužívá žádné triky a vypadá následovně:

$$P \implies T_1 \implies T_2 \implies \cdots \implies T_n \implies T.$$

Pokud jsme nikde během důkazu neudělali chybu, tak jsou všechny tyto implikace pravdivé. Takže pokud byly pravdivé naše předpoklady, tak musí být pravdivá i všechna tvrzení $T_1, \ldots T_n$ a konečně i T.

Tvrzení. *Pro všechna $x, y \in \mathbb{R}$ platí $|xy| \leq x^2 + y^2$.*

Toto tvrzení bychom mohli přepsat na implikaci $x, y \in \mathbb{R} \Rightarrow |xy| \leq x^2 + y^2$.

Důkaz. Víme, že pro všechna $a, b \in \mathbb{R}$ platí $(a-b)^2 \geq 0$. Takže speciálně platí i

$$(|x| - |y|)^2 \geq 0 \implies 0 \leq |x|^2 - 2\,|x|\,|y| + |y|^2 \implies 2\,|xy| \leq x^2 + y^2.$$

Současně platí $|xy| \leq 2\,|xy|$, z čehož vyplývá $|xy| \leq x^2 + y^2$.

❑

3.2 Důkaz sporem

Myšlenka důkazu sporem je strašně jednoduchá. Řekněme, že se snažíme dokázat nějaký výrok A, ale nejde nám to. Tak si zkusíme připustit, že možná neplatí, začneme předpokládat platnost $\neg A$ a ukážeme, že z toho plyne nějaký spor. Pokud jsme během důkazu neudělali žádnou chybu, tak máme pravdivou implikaci $\neg A \Rightarrow 0$. Z toho plyne, že výrok $\neg A$ je nepravdivý, takže A je pravdivý.

Definice. *Nechť $a, b \in \mathbb{Z}$. Pokud číslo a celočíselně dělí b, potom píšeme $a \mid b$. Formálně $a \mid b \equiv \exists q \in \mathbb{Z} : aq = b$.*

Definice. *Největší společný dělitel (NSD) čísel $a, b \in \mathbb{Z}$ je největší takové $n \in \mathbb{N}$, že platí $(n \mid a) \wedge (n \mid b)$. Píšeme $\mathrm{NSD}(a, b) = n$.*

Definice. *Čísla $a, b \in \mathbb{Z}$ jsou nesoudělná $\equiv \mathrm{NSD}(a, b) = 1$; zlomek $\frac{a}{b}$ nelze zkrátit.*

Lemma. *Pro všechna $n \in \mathbb{N}$ taková, že $\sqrt{n} \in \mathbb{Q}$, platí, že $\sqrt{n} \in \mathbb{N}$.*

Důkaz. Pro spor předpokládejme $\sqrt{n} \notin \mathbb{N}$. Víme, že $\sqrt{n}$ je nějaký kladný zlomek. Proto existují nesoudělná čísla $a, b \in \mathbb{N}$ splňující

$$\sqrt{n} = \frac{a}{b} \implies n = \frac{a^2}{b^2}.$$

Protože a a b jsou nesoudělná, tak jsou nesoudělná i a^2 a b^2. Navíc $n \in \mathbb{N}$, takže musí platit $b^2 = 1$, tedy $b = 1$ a $\sqrt{n} = a \in \mathbb{N}$. Ale předpokládali jsme, že $\sqrt{n} \notin \mathbb{N}$, což je spor. Náš předpoklad tedy musel být špatný, z čehož plyne $\sqrt{n} \in \mathbb{N}$. ❑

Implikace $\mathrm{NSD}(a,b) = 1 \Rightarrow \mathrm{NSD}(a^2,b^2) = 1$ vůbec není tak samozřejmá, jak se zprvu může zdát. Vyplyne až z vět o prvočíslech, které dokážeme v sekci 3.5.

Úloha. Dokažte tuto implikaci sporem pomocí základní věty aritmetiky a Euklidova lemmatu.

3.3 Důkaz obměnou

Obměna implikace $A \Rightarrow B$ je výrok $\neg B \Rightarrow \neg A$. Všimněme si, že obměna platí právě tehdy, když platí původní výrok. Takže místo toho, abychom dokazovali „*Když prší, tak je mokro.*“, tak dokážeme „*Když není mokro, tak neprší.*“, protože to třeba může být jednodušší.

Věta. *Pro všechna $n \in \mathbb{N}$ taková, že $\nexists k \in \mathbb{N} : n = k^2$ platí $\sqrt{n} \notin \mathbb{Q}$.*

Důkaz. Tato věta tvrdí, že pokud n není druhou mocninou nějakého přirozeného čísla, potom je $\sqrt{n}$ iracionální. Dokázat toto tvrzení přímo nebo sporem by bylo velmi obtížné, proto zkusíme vyslovit obměnu a místo výroku

$$\nexists k \in \mathbb{N} : n = k^2 \implies \sqrt{n} \notin \mathbb{Q}$$

se pokusíme dokázat výrok

$$\sqrt{n} \in \mathbb{Q} \implies \exists k \in \mathbb{N} : n = k^2.$$

Protože $\sqrt{n} \in \mathbb{Q}$ a navíc $n \in \mathbb{N}$, tak nám předchozí lemma garantuje, že $\sqrt{n} \in \mathbb{N}$. Čili hledané k je $\sqrt{n}$.

❑

Důsledek. Pokud odmocnina přirozeného čísla není jiné přirozené číslo, potom je iracionální.

Poznámka. Pro $n = 2$ je tuto větu možné dokázat bez obměny, a sice sporem.

3.4 Důkaz matematickou indukcí

Matematická indukce nám umožňuje dokazovat některá tvrzení ve tvaru

$$\forall n \in \mathbb{N}, n \geq n_0 : \varphi(n),$$

kde $n_0 \in \mathbb{N}$ a φ je nějaké logická formule s jednou volnou proměnnou. Myšlenka indukce je taková, že místo toho, abychom dokazovali platnost φ pro všechna n najednou, tak to uděláme postupně. Nejprve ověříme platnost $\varphi(n_0)$ a potom dokážeme

$$\forall n \in \mathbb{N}, n \geq n_0 : \varphi(n) \implies \varphi(n+1).$$

Tomuto výroku se říká indukční hypotéza a platnost $\varphi(n)$ nazýváme indukční předpoklad. Takže pokud platí $\varphi(0)$, potom platí i $\varphi(1)$. A pokud platí $\varphi(1)$, potom platí i $\varphi(2)$ atd. Pojďme nyní sporem dokázat, že matematická indukce funguje.

Lemma. *Pokud* $\varphi(n_0)$ *a navíc* $\forall n \geq n_0 : \varphi(n) \Rightarrow \varphi(n+1)$*, potom* $\forall n \geq n_0 : \varphi(n)$*.*

Důkaz. Pro spor předpokládejme, že $\exists n \geq n_0 : \neg\varphi(n)$. Označme k nejmenší takové n. Potom buď $k = n_0$, což je spor s tím, že platí $\varphi(n_0)$, nebo $k > n_0$. Víme, že implikace $\varphi(k-1) \Rightarrow \varphi(k)$ platí a $\varphi(k)$ neplatí. Aby toto mohla být pravda, tak musí $\varphi(k-1)$ také neplatit. To je ale spor s tím, že k je nejmenší takové $n \geq n_0$, že $\varphi(n)$ neplatí.

❑

Matematická indukce tedy funguje. Vyzkoušíme si ji na jednoduchém příkladu.

Tvrzení. *Pro všechna* $n \in \mathbb{N}$ *platí* $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$*.*

Důkaz. Nejprve si ověřme, že to platí pro $n = 0$. Máme $2^0 = 2^1 - 1$, což je pravda. Nyní pojďme dokázat indukční hypotézu. Budeme dokazovat výrok

$$1 + 2 + \cdots + 2^n = 2^{n+1} - 1 \implies 1 + 2 + \cdots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Podle indukčního předpokladu máme

$$(1 + 2 + \cdots + 2^n) + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1.$$

Indukční hypotéza je tedy pravdivá, takže původní výrok je také pravdivý.

❑

Tato forma matematické indukce většinou stačí, ale občas je potřeba použít takzvanou *silnou* indukci.

3.5 Důkaz silnou matematickou indukcí

Princip silné indukce je úplně stejný jako indukce obyčejné, ale má mnohem silnější indukční krok, konkrétně

$$\forall n \in \mathbb{N}, n \geq n_0 : (\forall k \in \mathbb{N},\, n_0 \leq k \leq n : \varphi(k)) \implies \varphi(n+1).$$

Takže místo toho, abychom v indukčním kroku předpokládali, že platí pouze $\varphi(n)$, tak předpokládáme platnost všech doposud dokázaných výroků.

Definice. *Číslo $n \in \mathbb{N}$ je prvočíslo $\equiv n > 1$ a navíc n je dělitelné pouze jedničkou a samo sebou. Prvních pár prvočísel je* $2, 3, 5, 7, 11, \ldots$

Tvrzení. *Každé $n \in \mathbb{N}, n \geq 2$ je možné rozložit na součin prvočísel.*

Důkaz. Obyčejná indukce je na toto tvrzení krátká, protože rozklad čísla n nám neříká nic o rozkladu čísla $n+1$. Proto použijeme silnou indukci. Tvrzení zjevně platí pro $n = 2$. Nyní předpokládejme, že jsme tvrzení již dokázali pro všechna k, t.ž. $2 \leq k < n$ pro nějaké dané n, a pokusme se najít prvočíselný rozklad pro n. Pokud je n prvočíslo, potom $n = n$ je hledaný rozklad. V opačném případě existují přirozená čísla a, b, t.ž. $2 \leq a, b < n$ a $n = a \cdot b$. Podle indukčního předpokladu lze a i b rozložit na součin prvočísel. Součin těchto dvou součinů je hledaný rozklad pro n.

❑

Lemma (Euklidovo)**.** *Pokud nějaké prvočíslo dělí součin dvou celých čísel, potom dělí i některé z těchto čísel. Ekvivalentně: pokud nedělí první, pak dělí druhé.*

Euklidovo lemma je jedno z těch tvrzení, která vypadají strašně nevinně, ale vůbec není snadné je dokázat. Nejprve si předvedeme intuitivní, ale chybný důkaz.

Důkaz. Je všeobecně známo, že každé číslo lze jednoznačně rozložit na součin prvočísel. Takže pokud $p \mid ab$, potom p je některé z prvočísel v rozkladu čísla ab. Rozklad čísla ab je ovšem pouze součin rozkladů čísel a a b, takže p musí být v rozkladu některého z nich. Proto $p \mid a$ nebo $p \mid b$.

❑

Tento důkaz je nefunguje, protože ačkoliv je tvrzení, že každé číslo má *jednoznačný* prvočíselný rozklad pravdivé, tak vyplývá právě z Euklidova lemmatu. Takže vlastně říkáme, že Euklidovo lemma platí, protože platí Euklidovo lemma.

My pomocí silné indukce dokážeme trochu obecnější verzi tohoto lemmatu. Všimněme si, že prvočíslo p nedělí číslo a právě tehdy, když $\mathrm{NSD}(p, a) = 1$.

Lemma. *Nechť $p, a, b \in \mathbb{Z}$. Pokud $p \mid ab$, ale* $\mathrm{NSD}(p, a) = 1$*, potom $p \mid b$.*

Důkaz. Případ $ab = 0$ je triviální, jelikož všechno dělí nulu. Bez újmy na obecnosti předpokládejme $p, a, b > 0$, tedy $ab > 0$. Tvrzení dokážeme silnou indukcí podle ab. Základní případ naší indukce bude $ab = 1 \cdot 1$. Nyní předpokládejme, že jsme tvrzení již dokázali pro všechny menší hodnoty, než nějaké dané ab. Protože $p \mid ab$, tak $\exists n \in \mathbb{N} : pn = ab$. Mohou nastat tři případy.

1. Pokud $p = a$, potom $p = 1$, protože $\mathrm{NSD}(p, a) = 1$. Takže určitě $p \mid b$.

2. Pokud $p < a$, potom zkoumejme součin

$$p(n-b) = (a-p)b \iff pn - pb = ab - pb \iff pn = ab.$$

Zřejmě $p \mid (a-p)b$. Označme $d \coloneqq \mathrm{NSD}(p, a-p)$. Určitě $d \mid (p + (a-p))$, takže $d \mid a$. Navíc $d \mid p$, ale $\mathrm{NSD}(p,a) = 1$, z čehož plyne $d = 1$. Takže $\mathrm{NSD}(p, a-p) = 1$ a protože $1 \leq (a-p)b < ab$, tak z indukční hypotézy víme, že $p \mid b$.

3. Pokud $p > a$, tak obdobně zkoumejme součin

$$(p-a)n = a(b-n) \iff pn - an = ab - an \iff pn = ab.$$

Zřejmě $(p-a) \mid a(b-n)$. Ze stejné argumentace jako v případě 2. vyplývá $\mathrm{NSD}(p-a, a) = 1$ a protože $1 \leq a(b-n) < ab$, tak z indukční hypotézy máme $(p-a) \mid (b-n)$. Tedy $\exists k \in \mathbb{N} : b - n = k(p-a)$. Dosazením do rovnice výše získáme

$$(p-a)n = ak(p-a) \implies n = ak \implies ab = pn = pak \implies b = pk.$$

Jelikož $b = pk$ pro nějaké $k \in \mathbb{N}$, tak $p \mid b$.

Ve všech případech jsme dospěli k závěru $p \mid b$, což dokazuje indukční hypotézu a tedy i celé tvrzení.

❑

Věta (Základní věta aritmetiky)**.** *Prvočíselný rozklad je až na pořadí činitelů vždy jednoznačný.*

Důkaz. Pro spor předpokládejme, že existuje nějaké číslo se dvěma různými rozklady. Označme n nejmenší takové číslo; tedy $n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$. Protože $p_1 \mid n$, tak $p_1 \mid (q_1 \cdots q_k)$ a podle Euklidova lemmatu $p_1 \mid q_i$ pro nějaké i. Jelikož nezáleží na pořadí činitelů, tak bez újmy na obecnosti buď $q_i = q_1$. Poněvadž p_1 i q_1 jsou prvočísla, tak $p_1 = q_1$, takže $p_2 \cdots p_j = q_2 \cdots q_k$, což nám dává dva různé rozklady pro nějaké číslo menší než n, a to je spor s minimalitou n.

❑

Na tento důležitý poznatek ještě narazíme. Je také mimochodem tím důvodem, proč nechceme, aby jednička byla prvočíslem. Protože potom by například $2 \cdot 3$ a $1 \cdot 2 \cdot 3$ byly dva různé rozklady čísla 6.

Poznámka. Základní větu aritmetiky lze dokázat i bez Euklidova lemmatu, takže kdybychom to udělali, tak by ten chybný důkaz Euklidova lemmatu uvedený výše fungoval.

4 Naivní teorie množin

Pojmem „naivní teorie“ myslíme teorii, která není formálně popsaná, tedy není jasné, jaké má axiomy. Místo toho se na její popis používá přirozený jazyk. Na množiny se dívá jako na soubory (kolekce) libovolných „věcí“. Tento přístup je velmi intuitivní a v naprosté většině případů zcela dostačující. Běžně se v matematice pohlížíme na množiny tímto naivním způsobem a ničemu to nevadí. Ale ukáže se, že to občas vede k paradoxům. Cantor také svoji teorii formuloval tímto „naivním“ způsobem.

4.1 Co je to množina?

Původní myšlenka byla, že množina může obsahovat úplně cokoliv, co si dokážeme představit. Nejsou vůbec žádná omezení. Nejjednodušší způsob jak vyrobit nějakou množinu je výčtem jejích prvků. Například

$$\{1, 2, 3\}, \quad \{\textit{pes, kočka}\}, \quad \{\textit{mladý, starý, krásný, dlouhý}\}.$$

To ale není moc zajímavé. Další způsob, jak popsat, co by v naší množině mělo být, je specifikovat nějakou charakteristickou vlastnost všech jejích prvků. Pro to používáme zápis ve tvaru $\{x \mid \varphi(x)\}$. Znamená, že chceme vytvořit množinu, která bude obsahovat všechny „věci“, které splňují logickou formuli φ. Například

$$\{x \mid x \textit{ je prvočíslo}\}, \quad \{x \mid x \textit{ je pes}\}, \quad \{x \mid x \textit{ je lidská vlastnost}\}.$$

Potom množina $\{x \mid x \textit{ je pes}\}$ je množina všech psů. Pokud máte psa, potom je v této množině. Hurvínkův pes Žeryk je také v této množině, přestože ve skutečnosti neexistuje. Pokud naše množina neobsahuje žádné prvky, potom ji nazýváme *prázdnou* a značíme ji $\varnothing$. Množiny samozřejmě mnohou obsahovat i jiné množiny. Například

$$\{x \mid x \textit{ je množina obsahující právě čtyři prvky}\}$$

je množina všech čtyř-prvkových množin. Dokonce můžeme vyrobit množinu všech množin jako $\{x \mid x \textit{ je množina}\}$. Je vidět, že tento zápis je velmi mocný.

Dále bychom si měli ujasnit, kdy jsou dvě množiny identické. Záleží nám pouze na tom, které věci v dané množině jsou, pořadí ani počet opakování těchto věcí pro nás nejsou důležité. Takže množiny

$$\{1, \{2\}\}, \quad \{\{2\}, 1\}, \quad \{1, \{2\}, \{2\}\}, \quad \{1, \{2\}, \{2, 2\}\}$$

jsou všechny identické. Počtem prvků množiny myslíme počet *unikátních* prvků. Takže všechny tyto množiny mají právě dva prvky, a sice 1 a $\{2\}$.

Přestože Cantor svoji teorii nikdy nepředvedl do axiomů, tak my si můžeme představovat, že má jeden jediný axiom, který říká, že všechno je množina.

Axiom. *Pro každou logickou formuli $\varphi(x)$ existuje množina $\{x \mid \varphi(x)\}$.*

Správně bychom měli ještě přidat nějaký axiom hovořící o identitě dvou množin, ale to prozatím zameteme pod koberec a budeme identitu vnímat tak, jak jsme si ji definovali výše.

4.2 Operace s množinami

Množiny určitě budeme chtít umět sjednocovat, dívat se které prvky mají společné a nějak je porovnávat. Pojďme to nadefinovat pořádně.

Definice. *Množina A je podmnožinou množiny $B \equiv \forall x \in A : x \in B$.*
Tento vztah zapisujeme jako $A \subseteq B$.

Ukázka. $\{1,2\} \subseteq \{1,2,3\}$, ale $\{4\} \nsubseteq \{1,2,3\}$, protože $4 \notin \{1,2,3\}$. Všimněme si, že každá množina je svojí vlastní podmnožinou a že prázdná množina $\varnothing$ je podmnožinou každé množiny. Tedy, pro každou množinu A platí $\varnothing \subseteq A$ a $A \subseteq A$.

Pozorování. Pokud $A \subseteq B$ i $B \subseteq A$, potom $A = B$.

Definice. *Potenční množina množiny A je množina všech jejích podmnožin*

$$\mathcal{P}(A) \coloneqq \{x \mid x \subseteq A\}.$$

Potenční množinu budeme značit jako $\mathcal{P}(A)$, ale někdy se používá i značení 2^A.

Ukázka. $\mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

Definice. *Sjednocení množin A a B je množina $A \cup B \coloneqq \{x \mid x \in A \vee x \in B\}$.*

Ukázka. $\{1,2\} \cup \{3,4\} = \{1,2,3,4\}$ a $\{1,2\} \cup \{1,4\} = \{1,2,4\}$.

Definice. *Průnik množin A a B je množina $A \cap B \coloneqq \{x \mid x \in A \wedge x \in B\}$.*

Ukázka. $\{1,2\} \cap \{3,4\} = \varnothing$ a $\{1,2\} \cap \{1,4\} = \{1\}$.

Dobrá mnemotechnická pomůcka pro zapamatování si, který oblouček znamená co je následující. $\cup \sim \vee$ a $\cap \sim \wedge$.

4.3 Přirozená čísla v naivní teorii množin

Zdroje VIDEO a WIKI.
Emanuel Kant – Matematika je konstruktem lidské mysli.
Russell a Frege – Matematika je objektivní, je to odvětví logiky

Frege založil predikátovou logiku ve své knize Begriffsschrift roku 1879. Pokusil se popsat všechny koncepty aritmetiky pomocí logiky a teorie množin, roku 1893 první vydání. Frege a Russell chtěli definovat přirozená čísla jako množiny. Číslo n by byla množina všech n-prvkových množin.

Druhé vydání mělo vyjít roku 1903, ale Russel mu roku 1902 poslal dopis, kde představil paradox, který bylo možné sestrojit ve Fregově systému. Fregem to otřáslo a v dodatku této knihy napsal

> Hardly anything more unfortunate can befall a scientific writer than to have one of the foundations of his edifice shaken after the work is finished. This was the position I was placed in by a letter of Mr. Bertrand Russell, just when the printing of this volume was nearing its completion.

Russel nakonec Fregu přesvědčil, že problém není v jeho logice, ale v teorii množin.

4.4 Russelův paradox

Russellův paradox, také známý jako paradox holiče, zní následovně: „Holič holí všechny muže ve městě, kteří neholí sami sebe. Kdo holí holiče?“. Pokud holiče holí holič, potom holič holí sám sebe, takže holiče holič neholí. Naopak, pokud holiče neholí holič, potom holič neholí sám sebe, takže jej holí holič. V obou případech jsme dospěli k logickému paradoxu. Matematicky můžeme Russellův paradox vyjádřit pomocí krotkých a divokých množin.

Definice. *Množina M je*

1. *krotká $\equiv M \notin M$; tedy M neobsahuje sama sebe jako prvek.*
2. *divoká $\equiv M \in M$; tedy M obsahuje sama sebe jako prvek.*

Například *množina všech zvířat* je krotká, protože to je množina a ne zvíře. Na druhou stranu, *množina všech věcí, které nejsou čajové lžičky* je divoká. Tato množina totiž obsahuje úplně všechno, co není čajová lžička. Je to množina, takže to není čajová lžička, proto obsahuje sama sebe. *Množina všech věcí, na které právě myslím* je většinou krotká, ale právě teď, když píšu tuto větu, je divoká. Podívejme se na množinu všech krotkých množin $M \coloneqq \{x \mid x \text{ je krotká}\}$. Je krotká nebo divoká?

- Pokud je krotká, potom splňuje definiční podmínku M, tedy $M \in M$, takže je divoká.
- Pokud je divoká, potom nesplňuje definiční podmínku M, tedy $M \notin M$, takže je krotká.

Tato množina je krotká právě tehdy, když je divoká, což je spor. Z toho vyplývá, že naivní teorie množin je sporná a musí být něco špatně s předpokladem, že existují úplně všechny množiny.

Russellův paradox jako první zřejmě objevil matematik Ernst Zermelo v roce 1899, ale své zjištění nezveřejnil. Publikoval ho až Russell v roce 1901. Návrh první axiomatické teorie, která se tomuto paradoxu snažila vyhnout, přišel od Zermela roku 1908. Matematik Abraham Fraenkel ovšem roku 1921 poukázal na to, že v Zermelově teorii není možné dokázat existenci některých množin, jejichž existenci většina tehdejších množinových teoretiků považovala za samozřejmou. Následující rok navrhl úpravu axiomů této teorie, čímž vznikla dnes velmi rozšířená Zermelo-Fraenkelova teorie množin (ZF).

Další známý paradox v naivní teorii množin se týká množiny všech množin. Předpokládáme, že existuje úplně libovolná množina, takže existuje i množina všech množin. Později ovšem dokážeme, že množina všech množin neexistuje.

5 Zermelo-Fraenkelova teorie množin

Zdroje: Archiv prasátka, Wiki a NAIL062.

Až doposud mohly množiny obsahovat libovolné „věci“ a vlastně jsme nijak nespecifikovali, co přesně jsou tyto věci zač. V axiomatické teorii množin existují pouze ty objekty, jejichž existence vyplývá z axiomů dané teorii. Axiomy ZF nám garantují existenci prázdné množiny a poskytují nám několik způsobů jak z již existujících množin vyrábět nové. Jinými slovy – všechno je množina. Každý prvek každé množiny je jen nějaká jiná množina.

5.1 Množiny a třídy

Jak jsme již konstatovali (a jak dokážeme), množina všech množin neexistuje. Ale chtěli bychom aby existovalo něco podobného, protože občas chceme mluvit o kolekci všech objektů, které něco splňují, přestože to už není množina. Proto se zavádí pojem *třída*. V naivní teorii množin je třída a množina jedno a totéž. Pokud omezíme co všechno může být množinou, tak se náš svět rozdělí.

- Množiny – někam náleží
- Třídy – něco náleží do nich

Všimněme si, že každá množina je zároveň i třídou. Opačně to ale platit nemusí, například třída všech množin není množinou. Takové třídě, říkáme *vlastní třída*. Uvědomme si, že tento koncept neumožňuje zrekonstruovat Russellův paradox, jelikož třída všech krotkých tříd zjevně neexistuje. Třídy totiž nemohou nikam náležet, věci pouze náleží do nich.

5.2 Co je to teorie?

Problém: Pro definování logiky prvního řádu potřebujeme množiny, ale pro vyjádřeni teorie množin potřebujeme logiku prvního řádu.

Řešení: Většina konceptů logiky stojí na řetězcích znaků přirozeného jazyka. Například relace se dají definovat i bez množin. Jazyk je seznam symbolů, které smíme používat. Formule jsou nápisy v nějakém jazyce, které se tvoří podle určitých pravidel. Teorie je opět nějaký seznam nápisů. V teorii můžeme dokazovat tvrzení, protože to jsou zase jen další nápisy. Axiomy teorie určují chování relačních a funkčních symbolů toho jazyka. Kdybychom chtěli nějaký konkrétní model té teorie, tak už potřebujeme množiny.

Když jsme si v kapitole o jazyku matematiky představovali některé pojmy z logiky, tak jsme letmo zmínili o pojem *teorie*. Řekli jsme, že teorie je nějaká množina axiomů a většinu detailů jsme zametli pod koberec. Pojďme si nyní pojem teorie představit trochu exaktněji. Pro další práci s množinami to nebude příliš podstatné, ale může to změnit náš pohled na význam axiomů, které se rozhodneme do naší teorii přidat.

- **Signatura** je dvojice $\langle \mathcal{R}, \mathcal{F} \rangle$, kde $\mathcal{R}$ je seznam relačních symbolů a $\mathcal{F}$ je seznam funkčních symbolů spolu s jejich aritami. Funkcím arity 0 říkáme konstanty. Symbol ‘=’ je rezervovaný pro rovnost. Signatura množin obsahuje pouze jediný relační symbol a vypadá takto: $\langle \in \rangle$. Signatura je tedy pouze nějaký nápis.

- **Struktura** v signatuře $\langle \mathcal{R}, \mathcal{F} \rangle$ je trojice $\langle \mathcal{A}, \mathcal{R}^{\mathcal{A}}, \mathcal{F}^{\mathcal{A}} \rangle$, kde $\mathcal{A}$ je nějaká neprázdná třída, říkáme jí *doména* nebo *univerzum* této struktury. $\mathcal{R}^{\mathcal{A}}$ a $\mathcal{F}^{\mathcal{A}}$ jsou množiny konkrétních relací a funkcí, které realizují symboly odpovídající signatury. Takže struktura je nějaká konkrétní „implementace“ signatury, pro jejíž popsání už potřebujeme množiny.

- **Jazyk** je seznam symbolů, ze kterých budeme moci stavět výroky, a vztahuje k nějaké konkrétní signatuře. Jazyk potom obsahuje relační a funkční symboly této signatury. Dále musíme přidat informaci, zda to je jazyk s *rovností* nebo ne. V jazyku s rovností můžeme používat symbol '=', který vyjadřuje identitu prvků z domény nějaké konkrétní struktury dané signatury. V každém jazyce (nezávisle na signatuře) jsou také symboly, které nám umožňují vytvářet logické formule. To znamená například symboly pro logické spojky ($\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$), kvantifikátory ($\forall, \exists$), proměnné ($x, y, z, \dots$) a závorky '(' a ')'.

  Pokud jazyk obsahuje rovnost, tak nám opravdu umožňuje rozhodnout, zda jsou dva prvky v nějaké konkrétní struktuře identické. Pokud bychom si vzali jazyk bez rovnosti, který by měl relační symbol '$=_R$' (symbol '=' je rezervovaný pro skutečnou rovnost) a nadefinovali jsme pomocí něj identitu dvou prvků, tak by se to chovali jinak. Podrobněji tento rozdíl uvidíme u axiomu extenzionality.

  Jazyk teorie množin je $\langle \in \rangle$ s rovností.

- **L-formule** je nějaký nápis ze symbolů jazyka L splňující určitá pravidla. Tyto pravidla zajišťují, že formule dávají dobrý logický smysl. Například, pokud je φ formule, potom je $(\neg\varphi)$ také formule.

- **Teorie** jazyka L je seznam L-formulí, kterým říkáme axiomy. V teorii můžeme z axiomů dokazovat pravdivost jiných L-formulí.

  Model teorie T je libovolná struktura jazyka L, která splňuje všechny axiomy T. Je to nějaká konkrétní realizace té teorie. Protože všechno co jsme v T dokázali vyplývá z axiomů, tak to platí i v každém modelu T. Čili dokazovat věci v T můžeme bez množin, ale abychom se mohli bavit o nějakém konkrétním modelu T, tak množiny potřebujeme.

Další příklad teorie, se kterou se ještě setkáme je teorie reálných čísel. Po zhroucení geometrické interpretace matematické analýzy bylo potřeba vymyslet nějaký formální systém, ve kterém by se všechno dokazovalo. Matematici sepsali seznam vlastností, která chtějí aby reálná čísla měla (axiomy) a na základě těchto vlastností dokazují všechno ostatní. Signatura reálných čísel je stejná jako každého jiného uspořádaného tělesa, tedy $\langle +, -, 0, \cdot, 1, \leq \rangle$, kde $+$ a $\cdot$ jsou binární funkční symboly, $-$ je unární funkční, 0 a 1 jsou konstantní symboly a $\leq$ je binární relační symbol. Axiomy reálných čísel zajišťují, že symboly $+$, $-$, $\cdot$ a $\leq$ se chovají tak, jak bychom čekali; např. $x + y = y + x$ nebo $x < y \Rightarrow x + z < y + z$. A poslední, nejdůležitější axiom říká, že každá neprázdná, shora ohraničená podmnožina reálných čísel má nejmenší horní hranici, které říkáme supremum. Této vlastnosti se říká úplnost a zlomky ji nemají. V kapitole o důkazových technikách jsme dokázali, že mnoho odmocnin přirozených čísel není racionálních, takže racionální čísla jsou „děravá“.

Všechno o reálných číslech se tedy dokazuje z těchto axiomů a vlastní „implementace“ není důležitá.

5.3 Axiomy ZF

Nyní si polo-formálně představíme axiomy Zermelo-Fraenkelovy teorie množin. Nebude to zcela formální, protože správně bychom měli používat pouze symboly jazyka teorie množin, což znamená logické spojky, závorky, kvantifikátory, písmenka pro proměnné a relační symbol ‘$\in$’. Jazyk teorie množin je s rovností, takže máme k dispozici i symbol ‘$=$’. To znamená, že notace $\{x, y\}$ formálně nemá smysl. Ale z axiomů ZF ji lze formálně nadefinovat, takže ji budeme používat.

5.3.1 Axiom extenzionality

Axiom 1. *Množina není dána ničím jiným než svými prvky.*

$$((\forall z) : (z \in x \Leftrightarrow z \in y)) \implies (x = y).$$

Česky. Pokud pro množiny x a y platí, že každá množina z je prvkem x, právě tehdy, když je prvkem y, potom x je stejná jako y.

Je důležité zmínit, že toto *není* definice identity dvou množin. Musíme vnímat odděleně dva koncepty. První koncept je naše teorie, ve které můžeme dokazovat různá pravdivá tvrzení. Je to něco zcela abstraktního. Druhý koncept je nějaká konkrétní „implementace“ (model) této teorie. Symbol ‘$=$’ hovoří o identitě objektů, které poskytne ta konkrétní implementace. My „zevnitř“ naší teorie vůbec netušíme, jak by tato implementace mohla vypadat. Ale máme „zvenčí“ poskytnutý symbol $=$, který smíme používat. Každá implementaci „ví“, co tento symbol znamená. Ale neví, co znamená symbol $\in$. Axiomy jsou nějaké požadavky, které musí každý model splňovat. Takže tento axiom není definice identity dvou množin, protože identita je koncept, který je odtržený od teorie a přísluší až konkrétnímu modelu. Tento axiom vyjadřuje vztah symbolu $\in$ a identity a každý model bude muset tento požadavek splnit. K této myšlence se ještě vrátíme.

Opačná implikace

$$(x = y) \implies ((\forall z) : (z \in x \Leftrightarrow z \in y)).$$

platí také, ale není součástí axiomu extenzionality, protože vlastně říká

$$(\forall z) : (z \in x \Leftrightarrow z \in x),$$

což platí pro libovolnou implementaci symbolu $\in$.

5.3.2 Axiom prázdné množiny

Axiom 2. *Existuje prázdná množina, kterou budeme značit* $\varnothing$.

$$(\exists \varnothing) : (\forall x : x \notin \varnothing).$$

Česky. Existuje množina $\varnothing$ t.ž. každá množina x není prvkem množiny $\varnothing$.

5.3.3 Axiom dvojice

Axiom 3. *Pro každou dvojici množin x a y existuje množina d, která obsahuje právě x a y. Množinu d značíme jako $\{x, y\}$.*

$$(\forall x, y)(\exists d) : (\forall z)(z \in d \Leftrightarrow (z = x \vee z = y)).$$

Česky. Pro libovolnou dvojici množin x a y existuje množina d t.ž. libovolná množina z je prvkem d právě tehdy, když $z = x$ nebo $z = y$.

Tento axiom zaručuje i existenci jednoprvkových množin $\{x\} = \{x, x\}$.

5.3.4 Axiom sumy

Axiom 4. *Pro každou množinu x existuje množina s, která je sjednocením všech množin uvnitř x. Této množině říkáme suma množina x a značíme ji $\bigcup x$.*

$$(\forall x)(\exists s) : (\forall z)(z \in s \Leftrightarrow (\exists y \in x : z \in y)).$$

Česky. Pro každou množinu x existuje množina s t.ž. libovolná množina z je prvkem s právě tehdy, když množina x obsahuje nějakou množinu obsahující z.

Nyní můžeme pomocí kombinace axiomu sumy a axiomu dvojice definovat sjednocení dvou množin a libovolně velkou konečnou množinu danou výčtem.

Definice 1. *Sjednocení množin x a y definujeme jako $x \cup y \coloneqq \bigcup\{x, y\}$.*

Definice 2. *Množiny $\{x_1\}$ a $\{x_1, x_2\}$ jsou garantované axiomem dvojice. Množinu $\{x_1, x_2, \ldots x_n\}$ definujeme rekurzivně jako $\{x_1, x_2, \ldots x_{n-1}\} \cup \{x_n\}$.*

Ukázka. $\bigcup\big\{\{x_1\}, \{x_1, x_2\}, \{x_2, x_3\}\big\} = \{x_1, x_2, x_3\}$, $\bigcup \varnothing = \varnothing$.

5.3.5 Schéma axiomů specifikace

Schéma znamená, že se nejedná o jeden konkrétní axiom, ale o nekonečně mnoho různých axiomů, které mají všechny stejnou strukturu. V tomto případě je možné za $\varphi(z)$ dosadit libovolnou formuli, která neobsahuje symbol y.

Axiom 5. *Pokud je x množina a $\varphi(z)$ formule, potom existuje množina všech prvků z množiny x, které splňují φ. Tuto množinu značíme $\{z \in x \mid \varphi(z)\}$.*

$$(\forall x)(\exists y) : (\forall z)\big(z \in y \Leftrightarrow (z \in x \wedge \varphi(z))\big).$$

Česky. Pro každou množinu x existuje množina y t.ž. libovolná množina z je prvkem y právě tehdy, když z je prvkem x a navíc z splňuje formuli φ.

Všimněme si, že schéma axiomů specifikace nám nedovoluje vyrobit množinu všech množin nebo množinu všech krotkých množin, protože neumožňuje konstrukce typu $\{x \mid \varphi(x)\}$. Použitím axiomu vždy vznikne podmnožina nějaké již existující množiny.

Nyní také konečně můžeme nadefinovat průnik dvou množin a průnik množiny.

Definice 3. *Průnik dvou množin x a y je množina $x \cap y \coloneqq \{z \in x \mid z \in y\}$.*

Definice 4. *Množiny x a y jsou disjunktní $\equiv x \cap y = \varnothing$.*

Definice 5. *Průnik množiny x je množina* $\bigcap x \coloneqq \left\{z \in \bigcup x \,|\, \forall y \in x : z \in y\right\}$.

Ukázka. Průnik konečně mnoha množin $x_1, x_2, \ldots x_n$ lze zapsat dvěma způsoby:

$$\bigcap\{x_1, x_2, \ldots x_n\} = x_1 \cap x_2 \cap \cdots \cap x_n.$$

Průnik nekonečně mnoha množin už ovšem lze udělat pouze jako průnik nekonečné množiny x.

Poznámka. Při jiných definicích průniku množiny x se často uvádí podmínka, že x musí být neprázdná. Ovšem při této definici platí $\bigcap \varnothing = \bigcup \varnothing = \varnothing$, což je přijatelné chování.

5.3.6 Axiom potenční množiny

Připomeňme si, nyní trochu formálněji, definici podmnožiny.

Definice 6. *Zápis $y \subseteq x$ je zkratka pro formuli $\forall z \in y : z \in x$)*

Axiom 6. *Pro každou množinu x existuje množina p, která obsahuje všechny podmnožiny množiny x. Této množině říkáme potenční množina množiny x nebo potence x a značíme ji $\mathcal{P}(x)$.*

$$(\forall x)(\exists p) : (\forall z)(z \in p \Leftrightarrow z \subseteq x).$$

Česky. Pro každou množinu x existuje množina p t.ž. libovolná množina z je prvkem p právě tehdy, když z je podmnožinou x.

5.3.7 Axiom nekonečna

Nejprve definujeme zkratku pro následníka jako $\mathrm{Succ}(x) \coloneqq x \cap \{x\}$.

Axiom 7. *Existuje nekonečná množina s nějakou konkrétní strukturou.*

$$(\exists n) : (\varnothing \in n \wedge (\forall x)(x \in n \Rightarrow \mathrm{Succ}(x) \in n)).$$

Česky. Existuje množina n obsahující prázdnou množinu. Navíc má tato množina tu vlastnost, že pokud do ní náleží x, tak do ní náleží i následovník x.

Poznámka. Přesně takhle definujeme množinu všech přirozených čísel.

5.3.8 Schéma axiomů nahrazení

5.3.9 Axiom fundovanosti

Axiom 8. *Každá neprázdná množina obsahuje nějakou množinu, která je s ní disjunktní.*

$$(\forall x \neq \varnothing) : (\exists y \in x : x \cap y = \varnothing).$$

Důsledek. Neexistuje množina a splňující $a \in a$.

Důkaz. Pro spor nechť a je divoká. Potom množina $\{a\}$ nesplňuje fundovanost, protože $a \in a$ a zároveň $a \in \{a\}$, takže $a \in a \cap \{a\}$.

❑

Důsledek. Neexistuje dvojice množin a, b taková, že $a \in b$ a $b \in a$. Tentokrát poruší fundovanost množina $\{a, b\}$.

Tento axiom nám zaručuje, že v ZF nemůže vzniknout Russelův paradox, protože vylučuje možnost existence divokých množin.

Dále z tohoto axiomu vyplývá, že v ZF neexistuje množina všech množin, protože ta by určitě byla divoká, ale divoké množiny v ZF neexistují. Jenže tento argument neukazuje, proč množina všech množin neexistuje ani v naivní teorii množin.

6 Velikost nekonečných množin

6.1 Definice základních pojmů

Než se pustíme do matematiky teorie množin, tak budeme muset definovat některé základní pojmy, se kterými budeme pracovat.

Jako první definujeme uspořádanou dvojici, což je struktura, na které bude stát všechno ostatní. Budeme chtít, aby jednoznačně určovala svůj první i druhý prvek.

Definice 7. *Uspořádaná dvojice* (a, b) *je množina* $\{\{a\}, \{a, b\}\}$. *Uspořádanou* n*-tici* $(a_1, a_2, \dots a_n)$ *potom definujeme rekurzivně jako* $(a_1, (a_2, a_3, \dots a_n))$.

Pozorování. Nechť $p = (a, b) = \{\{a\}, \{a, b\}\}$. Označme P, resp. S průnik, resp. sjednocení množin uvnitř p. Všimněme si, že naše definice uspořádané dvojice jednoznačně určuje svůj první a druhý prvek jako

$$\{a\} = P, \quad \{b\} = \{x \in S \mid P \neq S \implies x \notin P\}.$$

Definice 8. *Kartézský součin dvou množin* A *a* B *je* $\{(a, b) \mid a \in A \wedge b \in B\}$. *Problém opět je, že jsme tento způsob konstrukce množin zakázali. Ale podle definice 7 je uspořádaná dvojice* (a, b) *množina, takže kartézský součin můžeme definovat ekvivalentně jako*

$$A \times B \coloneqq \{x \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid \exists a \in A\, \exists b \in B : x = (a, b)\}.$$

Kartézský součin n *množin* $A_1, A_2, \dots A_n$ *definujeme rekurzivně jako*

$$A_1 \times \cdots \times A_n \coloneqq A_1 \times (A_2 \times \cdots \times A_n) = \{(a_1, \dots a_n) \mid \forall i : a_i \in A_i\}.$$

Pokud jsou množiny $A_1, \dots A_n$ *stejné, potom jejich kartézský součin značíme* A^n.

Definice 9. *Binární relace* R *mezi množinami* A *a* B *je libovolná podmnožina* $A \times B$. *Píšeme* aRb *pokud* $(a, b) \in R$ *a čteme „*a *je v relaci* R *s* b*“. Pokud* $A = B$, *potom říkáme, že* R *je relace na* A.

Definice 10. *Binární relace* R *na množině* A *je*

1. *reflexivní* $\equiv \forall x \in A : xRx$,
2. *antisymetrická* $\equiv \forall x,y \in A, x \neq y : (xRy \implies \neg yRx)$,
3. *tranzitivní* $\equiv \forall x,y,z \in A : xRy \wedge yRz \implies xRz$,
4. *uspořádání na* $A \equiv R$ *je reflexivní, antisymetrická a tranzitivní.*

Definice 11 (ČUM)**.** *Částečně uspořádaná množina (ČUM) je uspořádaná dvojice* (A, R), *kde* A *je množina a* R *je nějaké uspořádání na* A. *Řekneme, že prvky* $x, y \in A$ *jsou porovnatelné, pokud* xRy *nebo* yRx.

Definice 12. *Každému uspořádání* $\leq$ *na množině* A *přiřadíme relaci* $<$ *na* A *definovanou jako* $\forall x,y \in A : x < y \equiv x \leq y \wedge x \neq y$. *Všimněme si, že* $<$ *není uspořádání, protože není reflexivní. Řekneme, že v ČUM* $(A, \leq)$ *je prvek* $x \in A$

1. *minimální* $\equiv \nexists y \in A : y < x$,
2. *nejmenší* $\equiv \forall y \in A : x \leq y$,
3. *maximální* $\equiv \nexists y \in A : x < y$,
4. *největší* $\equiv \forall y \in A : y \leq x$.

Pozorování. Pokud je nějaký prvek nejmenší, resp. největší, tak je i minimální, resp. maximální, ale obráceně to už platit nemusí. Podívejme se na třeba na relaci dělitelnosti $\mid$ na množině $\{1, \ldots 12\}$ definovanou jako $a \mid b \equiv a$ celočíselně dělí b a všimněme si, že to je uspořádání. Prvek 1 je nejmenší i minimální, protože cokoliv je dělitelné jedničkou. Prvky 7, 8, 9, 10, 11 a 12 jsou maximální, protože nedělí nic dalšího, ale žádný z nich není největší. Pokud by třeba prvek 12 měl být největší, potom by muselo platit $5 \mid 12$, což není pravda.

Definice 13. *Řekneme, že uspořádání $\leq$ na množině A je*

1. *lineární (úplné)* $\equiv$ *každé dva prvky A jsou porovnatelné pomocí $\leq$,*
2. *dobré* $\equiv$ *je lineární a navíc každá $B \subseteq A$ má nejmenší prvek vůči $\leq$,*
3. *husté* $\equiv \forall x, y \in A, x < y \; \exists z \in A : x < z < y$.

Pokud je $\leq$ lineární, resp. dobré uspořádání množiny A, tak říkáme, že $(A, \leq)$ je lineárně, resp. dobře uspořádaná množina.

Níže je uvedeno několik známých uspořádání a jejich vlastnosti.

- $(\mathbb{N}, \leq)$ Přirozená čísla se standardní interpretací $\leq$ jsou dobře uspořádaná množina. Její nejmenší prvek je nula.
- $(\mathbb{Z}, \leq)$ Standardní uspořádání celých čísel je úplné, ale není dobré, protože vůči $\leq$ neexistuje nejmenší celé číslo.
- $(\mathbb{Z}, \preceq)$ Uspořádání $x \preceq y \equiv (|x| < |y|) \vee (|x| = |y| \wedge x \leq y)$ celých čísel je dobré. Toto uspořádání vypadá následovně: $0, -1, 1, -2, 2, -3, 3, \ldots$
- $(\mathbb{Q}, \leq)$ Standardní uspořádání racionálních čísel je úplné a husté, ale není dobré, protože $\mathbb{Q}$ nemá žádný nejmenší prvek vůči $\leq$. Totéž platí pro $(\mathbb{R}, \leq)$. Dokonce ani nevíme, jestli nějaké dobré uspořádání reálných čísel existuje.
- $(\mathbb{N}^+, \mid)$ Přirozená čísla bez nuly spolu s relací dělitelnosti jsou částečné uspořádání. Toto uspořádání nemá žádný maximální prvek, ale zato má nejmenší prvek, a sice jedničku.
- $(\mathcal{P}(A), \subseteq)$ Potenční množina libovolné množiny A spolu s inkluzí je částečně uspořádané množina. V tomto uspořádání je prázdná množina $\varnothing$ nejmenší prvek a A největší prvek.
- $(\Sigma^*, \leq_{LEX})$ Lexikografické uspořádání konečných řetězců nad abecedou Σ je dobré uspořádání. Nejmenší prvek je prázdný řetězec. V pořadí tohoto uspořádání jsou seřazena například slova ve slovníku.

Definice 14. *Zobrazení (funkce) z množiny X do množiny Y je binární relace f mezi X a Y splňující*

$$(\forall x \in X)(\exists! y \in Y) : x f y,$$

tedy každý vzor má právě jeden obraz. Říkáme, že funkce f zobrazuje množinu X na množinu Y a píšeme $f : X \to Y$. Místo xfy píšeme $f : x \mapsto y$ nebo $f(x) = y$.

Kromě běžných matematických funkcí jako sinus, kosinus, polynomy atd. existuje sousta dalších užitečných funkcí. Například

- počet prvků spočetné množiny : $\mathcal{P}(\mathbb{N}) \to \mathbb{N} \cup \{\infty\}$,
- znaménková funkce $\operatorname{sgn} : \mathbb{R} \to \{-1, 0, 1\}, \quad x \mapsto \begin{cases} -1, & x < 0, \\ 0, & x = 0, \\ 1, & x > 0. \end{cases}$

Definice 15. *Zúžení funkce $f : A \to B$ na množinu $R \subseteq A$ je funkce*

$$f|_R : R \to B, \quad x \mapsto f(x).$$

Definice 16. *Funkce $f : X \to Y$ je*

1. *prostá (injekce)* $\equiv \forall x_1, x_2 \in X : x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$,
2. *na (surjekce)* $\equiv \forall y \in Y\ \exists x \in X : f(x) = y$,
3. *bijekce* $\equiv$ *je prostá a na, tedy* $\forall y \in Y\ \exists! x \in X : f(x) = y$.

Definice 17. *Posloupnost (a_n) je zobrazení $f : \mathbb{N} \to A$. Jde o zobecnění pojmu uspořádané n-tice pro nekonečné n. Píšeme $(a_n) \in A$.*

Definice 18. *Indexovaná rodina množin $(X_i)_{i \in I}$ je zobrazení $f : I \to X$, kde I je množina indexů a X je množina indexovaných množin.*

Definice 19. *Kartézský součin indexované rodiny množin $(X_i)_{i \in I}$ je*

$$\prod_{i \in I} X_i \coloneqq \left\{ f : I \to \bigcup_{i \in I} X_i \,|\, \forall i \in I : f(i) \in X_i \right\}.$$

Jde o zobecnění pojmu kartézského součinu pro libovolně mnoho množin.

6.2 Kardinalita

Kardinalita je něco jako velikost množiny. Kardinalitu konečné množiny definujeme jako počet jejích prvků. Takže kardinalita množiny $\{1, 2, 3\}$ je 3. Kardinalita nekonečných množin je trochu složitější. Určitě chceme, aby např. množina všech přirozených čísel měla větší kardinalitu než libovolná konečná množina. Ale současně chceme umět porovnávat kardinalitu různých nekonečných množin. Řekneme, že dvě množiny mají stejnou kardinalitu, pokud mezi nimi existuje bijekce. Tedy pokud můžeme prvky první množiny vzájemně jednoznačně spárovat s prvky druhé množiny.

Definice 20. *Kardinalitu (mohutnost) množiny A označíme $|A|$. Pro množiny A a B definujeme relace*

1. $|A| = |B| \equiv$ *existuje bijekce* $f : A \to B$,
2. $|A| \leq |B| \equiv$ *existuje prosté zobrazení* $f : A \to B$,
3. $|A| < |B| \equiv |A| \neq |B|$ *a současně* $|A| \leq |B|$.

Pokud $|A| = |B|$, tak píšeme $A \sim B$.

Pozorování. Pokud $A \subseteq B$, potom $|A| \leq |B|$.

Kardinalitám množin se říká kardinální čísla, jsou to $0 < 1 < 2 < \cdots < \aleph_0 < \aleph_1 < \aleph_2 < \cdots$. Kardinální čísla konečných množin jsou přirozená čísla. Přirozená čísla jsou $\mathbb{N} = \{0, 1, 2, \dots\}$. Zjevně jich je nekonečně mnoho, takže jejich kardinalita nemůže být žádné přirozené číslo. Proto zavedeme nové kardinální číslo $\aleph_0 := |\mathbb{N}|$. Dále definujeme $\aleph_{\alpha+1}$ jako nejmenší kardinální číslo větší než $\aleph_\alpha$. Dá se ukázat, že neexistuje žádné menší nekonečné kardinální číslo než $|\mathbb{N}|$, takže naše definice $\aleph_0$ je validní. Pořád jsme ale neukázali, že existuje kardinální číslo větší než $\aleph_0$.

6.3 Kardinalita přirozených čísel

Přestože se na první pohled může zdát, že sudých přirozených čísel je méně než všech přirozených čísel, tak to není pravda. Sudá čísla lze jednoznačně očíslovat například pomocí bijekce $f : n \mapsto 2n$. Pokud lze množinu očíslovat, potom říkáme, že je spočetná.

Definice 21. *Množina M je*

1. *spočetná* $\equiv |M| \leq |\mathbb{N}|$,
2. *spočetně nekonečná* $\equiv |M| = |\mathbb{N}|$.
3. *nespočetná* $\equiv |M| > |\mathbb{N}|$,

Možná poněkud překvapivé tvrzení je, že racionální čísla jsou spočetná. Tedy tvrdíme, že přirozených čísel je stejně jako všech zlomků.

Tvrzení 1. *Množina racionálních čísel $\mathbb{Q}$ je spočetně nekonečná.*

Důkaz. Podívejme se na zobrazení $f : \mathbb{Q} \to \mathbb{N}$, $f : \frac{a}{b} \mapsto 2^{|a|}\, 3^b\, 5^{1+\mathrm{sgn}(a/b)}$. Díky jednoznačnosti prvočíselného rozkladu přirozených čísel je f prostá, takže $|\mathbb{Q}| \leq |\mathbb{N}|$. Ale kardinalita racionálních čísel určitě nemůže být konečná, tedy $|\mathbb{Q}| = |\mathbb{N}|$. ❑

Toto tvrzení ještě zobecníme na něco mnohem mocnějšího. Všimněme si, že racionální čísla jsou vlastně uspořádané trojice (a, b, s), kde $a, b \in \mathbb{N}$ a $s \in \{-1, 0, 1\}$. Předchozí tvrzení vlastně říká, že množina všech těchto uspořádaných trojic je spočetná. Co kdyby to nebyly trojice, ale n-tice? Bude jich pořád spočetně mnoho? Nejprve ale budeme muset dokázat pomocné lemma hovořící o kardinalitě prvočísel.

Lemma 2. *Množina všech prvočísel $\mathbb{P}$ je spočetně nekonečná.*

Důkaz. $\mathbb{P} \subseteq \mathbb{N}$, takže $\mathbb{P}$ je spočetná. Stačí ukázat, že je nekonečná. Pro spor předpokládejme, že není. Potom existuje nějaké největší prvočíslo $p \in \mathbb{P}$. Nyní definujeme číslo P jako součin všech prvočísel plus jedna

$$P \coloneqq 1 + \prod_{q \in \mathbb{P}} q.$$

Všimněme si, že $\forall q \in \mathbb{P} : P \equiv 1 \pmod{q}$, takže P je prvočíslo a navíc $P > p$, což je spor s tím, že p je největší prvočíslo. ❑

Věta 3. *Kartézský součin konečně mnoha spočetných množin je spočetný.*

Důkaz. Označme dané množiny $A_1, A_2, \ldots A_n$ a jejich kartézský součin K. Dále definujme $A \coloneqq \{A_1, A_2, \ldots A_n\}$. Chceme udělat podobný argument jako v důkazu tvrzení 1, ale namísto prvočísel 2, 3 a 5 použít nějakých n prvočísel. Všechny zadané množiny jsou spočetné, tedy existuje očíslování jejich prvků přirozenými čísly. Označme φ_i číslovací funkci pro A_i. Zadaných množin je konečně mnoho, tedy existuje prosté zobrazení $\phi : A \to \mathbb{P}$. Nakonec definujme zobrazení

$$f : K \to \mathbb{N}, \quad f : (a_1, a_2, \ldots a_n) \mapsto \phi(A_1)^{\varphi_1(a_1)}\, \phi(A_2)^{\varphi_2(a_2)} \cdots \phi(A_n)^{\varphi_n(a_n)}.$$

Z toho, že zobrazení ϕ a číslovací funkce $\varphi_1, \varphi_2, \ldots \varphi_n$ jsou prosté, plyne, že zobrazení f je také prosté. Takže $|K| \leq |\mathbb{N}|$, tedy K je spočetný. ❑

Poznámka. Jiný způsob jak dokázat větu 3 je ukázat, že kartézský součin dvou spočetných množin je spočetný, z čehož lze tuto větu dokázat indukcí.

Pokud bychom měli spočetně nekonečně mnoho spočetných množin a každá z nich obsahovala alespoň dva prvky, potom by jejich kartézský součin už byl nespočetný. V další sekci toto tvrzení nepřímo dokážeme.

6.4 Kardinalita reálných čísel

Už je na čase položit si otázku, zda existuje nějaká množina s kardinalitou větší než mají přirozená čísla. Jednou takovou množinou jsou například reálná čísla. Je zajímavé, že racionální čísla jsou spočetná, ale když k nim přidáme i čísla iracionální, tak dostaneme nespočetnou množinu. Dokonce platí, že reálných čísel v libovolném intervalu je více než všech přirozených čísel.

Definice 22. *Interval je libovolná podmnožina reálných čísel $J \subseteq \mathbb{R}$ splňující*

$$|J| \geq 2 \quad \wedge \quad (\forall x,y \in J, x < y)(\forall z \in \mathbb{R}) : (x < z < y \implies z \in J).$$

Poznámka. Standardní definice intervalu jeho mohutnost nijak neomezuje, takže povoluje i „zdegenerované“ jednoprvkové a prázdné intervaly. Nám ale toto omezení usnadní život, protože nebudeme muset o každém intervalu explicitně říkat, že není zdegenerovaný.

Definice 23. *Řekneme, že podmnožina reálných čísel $G \subseteq \mathbb{R}$ je*

1. *zdola omezená* $\equiv (\exists a \in \mathbb{R})(\forall x \in G) : a \leq x$,
2. *shora omezená* $\equiv (\exists b \in \mathbb{R})(\forall x \in G) : x \leq b$,
3. *omezená* $\equiv$ *je zdola omezená i shora omezená.*

Tvrzení 4. *Množina reálných čísel je nespočetná, tedy $|\mathbb{R}| > |\mathbb{N}|$.*

Důkaz. Uvědomme si, že nám stačí vyvrátit existenci bijekce mezi reálnými čísly v intervalu $[0, 1)$ a přirozenými čísly, takže od tohoto okamžiku myslíme reálnými čísly tento interval. Pro naše účely bude jednodušší, pokud budeme o reálných číslech uvažovat ve dvojkové soustavě. Potom je pro nás reálné číslo prostě nějaká spočetně nekonečná posloupnost jedniček a nul. Označme $\varphi_i(x)$ i-tou číslici v této posloupnosti pro reálné číslo x.

Pro spor předpokládejme, že existuje bijekce $f : \mathbb{N} \to [0, 1)$. Sestrojíme nové reálné číslo r a ukážeme, že nemá vzor, takže f není bijekce. Číslo r definujeme tak, že určíme všechny jeho číslice jako $\varphi_i(r) \coloneqq 1 - \varphi_i(f(i))$. Lidskou řečí: pokud chci i-tou číslici r, tak se podívám na i-tou číslici i-tého reálného čísla a vezmu si její opak. Tím zajistíme, že r se liší od všech očíslovaných reálných čísel v alespoň jedné číslici, tedy $\forall n \in \mathbb{N} : f(n) \neq r$, což je spor s tím, že f je bijekce.

❑

Lemma 5. *Existuje bijekce $f : [0, 1) \to (0, 1)$.*

Důkaz. Chtěli bychom udělat identitu, ale nula by neměla obraz. Proto definujeme

$$f : x \mapsto \begin{cases} \frac{1}{2}, & x = 0, \\ \frac{1}{2^{n+1}}, & x = \frac{1}{2^n}, \quad n \in \mathbb{N}, \\ x, & \text{jinak.} \end{cases}$$

Čili $f(0) = 1/2, f(1/2) = 1/4, f(1/4) = 1/8$ atd. Ostatní prvky se zobrazí samy na sebe. Spočetnou množinu záporných mocnin dvojky jsme v podstatě „posunuli o jedna“, čímž nám vznikl nevyužitý obraz $1/2$, na který jsme zobrazili nulu.

❑

Pozorování. Podobným trikem lze ukázat $(0,1) \sim (0,1] \sim [0,1) \sim [0,1]$.

Důsledek. Všechny omezené intervaly reálných čísel mají stejnou mohutnost.

Důkaz. Existují čtyři druhy omezených intervalů, a sice (a,b), $(a,b]$, $[a,b)$ a $[a,b]$. Nejprve se zaměříme pouze na otevřené intervaly. Všimněme si, že zúžení lineární funkce $f|_{(a,b)}$ splňující $f(a) = c$ a $f(b) = d$ je bijekce mezi (a,b) a (c,d). Tedy $(a,b) \sim (0,1)$. Po zopakování tohoto procesu pro ostatní druhy omezených intervalů získáme $(a,b) \sim (a,b] \sim [a,b) \sim [a,b]$.

❑

Věta 6. *Všechny intervaly reálných čísel mají stejnou mohutnost jako* $\mathbb{R}$.

Důkaz. Už jsme ukázali, že všechny omezené intervaly reálných čísel mají stejnou mohutnost. Funkce tangens je bijekce mezi $(-\pi/2, \pi/2)$ a $\mathbb{R}$, takže omezené intervaly mají stejnou mohutnost jako $\mathbb{R}$. Nyní nechť I je libovolný omezený a J je libovolný neomezený interval. Všimněme si, že $|I| \leq |J|$, protože každý neomezený interval obsahuje nějaký omezený interval jako podmnožinu. Tedy platí $|\mathbb{R}| = |I| \leq |J| \leq |\mathbb{R}|$ z čehož plyne $|I| = |J| = |\mathbb{R}|$, což dokazuje tuto větu.

❑

Důkaz tohoto zásadního tvrzení byl poměrně zdlouhavý a nepříjemný. Později se budeme bavit o takzvaném axiomu výběru, pomocí kterého lze dojít ke stejnému výsledku mnohem snáz. Problém je, že axiom výběru nemusíme vždy považovat za pravdivý, takže by náš důkaz fungoval pouze v axiomatických systémech s axiomem výběru. Vlastně bychom dokázali nějakou méně univerzální pravdu.

6.5 Jak generovat velké množiny

Operace potenční množiny nám umožňuje vyrobit z libovolné stávající množiny nějakou jinou, větší množinu. Podívejme se na několik příkladů potenčních množin:

$$\begin{aligned}
\mathcal{P}(\varnothing) &= \{\varnothing\},\\
\mathcal{P}(\{1\}) &= \{\varnothing, \{1\}\},\\
\mathcal{P}(\{1,2\}) &= \{\varnothing, \{1\}, \{2\}, \{1,2\}\},\\
\mathcal{P}(\{1,2,3\}) &= \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.
\end{aligned}$$

Mělo by být vidět, že $\mathcal{P}(A)$ obsahuje mnohem více prvků než A a že $|\mathcal{P}(A)|$ je vždy nějaká mocnina dvojky.

Lemma 7. *Pro každou konečnou množinu* A *platí* $|\mathcal{P}(A)| = 2^{|A|}$.

Důkaz. Označme n mohutnost množiny A. Množina A je konečná, takže můžeme bez újmy na obecnosti předpokládat, že $A = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$. Každá podmnožina B množiny A je jednoznačně určena uspořádanou n-ticí nul a jedniček, kde jednička na k-té pozici znamená $k \in B$. Všimněme si, že tento vztah je vzájemně jednoznačný, takže počet všech podmnožin A je stejný jako počet těchto uspořádaných n-tic, což je 2^n.

❑

Tvrzení 8. *Reálná čísla a potenční množina přirozených čísel mají stejnou kardinalitu.*

Důkaz. V důkazu tvrzení 4 jsme o reálných číslech přemýšleli jako o nekonečných posloupnostech nul a jedniček. Dále, za použití podobného argumentu jako v důkazu lemmatu 7 můžeme libovolnou podmnožinu přirozených čísel popsat nekonečnou posloupnost nul a jedniček. Tedy existuje bijekce mezi reálnými čísly v intervalu $[0, 1)$ a podmnožinami přirozených čísel. A jak jsme již konstatovali výše, existuje bijekce $[0, 1) \to \mathbb{R}$. Z čehož plyne, že existuje bijekce $\mathcal{P}(\mathbb{N}) \to \mathbb{R}$, což dokazuje toto tvrzení.

❑

Víme, že $|\mathbb{N}| = \aleph_0$ a ukázali jsme $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$, tedy $|\mathbb{R}| \geq \aleph_1$. Bohužel nevíme, zda $|\mathbb{R}| = \aleph_1$. Tvrzení, že tato rovnost platí se nazývá hypotéza kontinua. Lze dokázat, že v současné standardní axiomatizaci matematiky není možné tuto hypotézu dokázat. Ekvivalentní tvrzení říká, že každá podmnožina reálných čísel je buď konečná, spočetně nekonečná, nebo má stejnou kardinalitu jako reálná čísla.

Viděli jsme, že potenční množina konečné množiny je větší než původní množina. Totéž platilo pro množinu přirozených čísel. Cantorova věta říká, že to platí obecně. Což nám umožňuje pomocí opakované aplikace potenční množiny konstruovat množiny se stále větší a větší kardinalitou.

Věta 9 (Cantorova)**.** *Pro každou množinu A platí $|A| < |\mathcal{P}(A)|$.*

Důkaz. Pro spor předpokládejme, že existuje bijekce $f : A \to \mathcal{P}(A)$. Definujme množinu $T \coloneqq \{a \in A \mid a \notin f(a)\}$. Nyní pro každý prvek a množiny A nastane jedna ze dvou situací:

$$a \in T \implies a \notin f(a) \implies T \neq f(a),$$
$$a \notin T \implies a \in f(a) \implies T \neq f(a).$$

V každém případě $T \neq f(a)$, takže T nemá vzor, což je spor s tím, že f je bijekce.

❑

Důsledek. Neexistuje žádné největší kardinální číslo.

Pomocí potenční množiny můžeme vyrábět neustále větší a větší množiny. Pokud začneme s nějakou konečnou množinou, tak můžeme aplikovat potenční množinu kolikrát chceme, ale její mohutnost zůstane konečná. Nejmenší nekonečné kardinální číslo $\aleph_0$ je zkrátka nedosažitelné z jakéhokoliv menšího kardinálního čísla. Ovšem, pokud už máme nějakou nekonečnou množinu, tak nám potenční množiny dovolují vyrábět pořád větší a větší nekonečné množiny.

Důsledek. Neexistuje množina všech množin.

Důkaz. Pro spor předpokládejme, že množina všech množin existuje a nazvěme ji M. Podle Cantorovy věty platí $|M| < |\mathcal{P}(M)|$. Ale M je množina všech množin, takže $\mathcal{P}(M) \subseteq M$, z čehož plyne $|\mathcal{P}(M)| \leq |M|$, což je spor.

❑